UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ENERO – JUNIO 2017

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

Ingeniería en Sistemas

PREVIO A LA OBTENCIÓN DEL TITULO DE

Ingeniera en Sistemas

TEMA:

Análisis de la seguridad informática en la red de datos entre sucursales de la empresa COMPUTER S.A de la ciudad de Babahoyo.

EGRESADA:

Iraida Graciela Lima Cerna

TUTOR:

Ing. Joffre León Acurio

AÑO 2017

INTRODUCCIÓN

De la información, en la actualidad la tecnología es el elemento fundamental para el desarrollo y la superación de los países, por lo que es necesario como un activo valioso, la misma que logra hacer que las organizaciones triunfen o quiebren, por lo que se debe ofrecer seguridad.

Existe el desconocimiento de las empresas por el tamaño del problema con el que se en ocasiones se están enfrentando, teniendo la consideración de la seguridad como aspecto secundario, dejando de invertir en la capacitación del capital humano, ni en el económico que es necesario para evitar o estar preparados para los daños y pérdidas de la información.

Las características principales que se verán afectadas por la amenaza en la seguridad como son la disponibilidad, integridad y confidencialidad pueden ser informaciones internas o externas, accidentalmente originadas o dejando a la organización con problemas con un fin perverso como por ejemplo las actividades se paralizarían dejando como resultado una cuantiosa pérdida dinero y tiempo de producción importantes factores de una organización para el desarrollo.

Las amenazas que afectan las características principales de la seguridad como son la confidencialidad, integridad y disponibilidad de la información pueden ser internas o externas, originadas accidentalmente o con un fin perverso dejando a la organización con problemas como por ejemplo la paralización de sus actividades que deja como resultado una perdida cuantiosa de tiempo de producción y dinero factores importantes para el desarrollo de una organización.

En la actualidad son varios los riesgos que en vista afectan en la seguridad de nuestras empresas y por lo tanto no es suficiente el capital con el que se cuenta para protegerlas esas vulnerabilidades debemos tenerlas controladas e identificadas y persiguiendo este objetivo se

logra que es la seguridad de la información, es que este proyecto se presenta es el Análisis de la seguridad informática en la red de datos entre sucursales de la empresa Computer S.A de la ciudad de Babahoyo.

En la actualidad los riesgos que afectan a la seguridad de las empresas son muchos, siendo así por lo general el capital que se determina para el control de lo mencionado no es suficiente, por lo que se debe considerar la identificación y control de las falencias. Esto con la persecución de objetivos que es la seguridad de la información, es que se presenta este proyecto es el Análisis de la seguridad informática.

DESARROLLO

COMPUTER S.A es considerada como una entidad de beneficio que directamente se encarga de las compras y ventas de los accesorios informáticos y equipos, además la prestación de los servicios de asesoramiento, mantenimiento y asistencia técnica a todos los usuarios externos.

Se mantendrá constituida como una institución ya que serán dos socios propietarios contando con dos sucursales ubicadas en la calle sucre, 10 de agosto y malecón y la otra en la calle Roldos y primer callejón, la otra en las calles. Será constituida como Sociedad Anónima ya que dos personas conformaran la organización.

La atención de los usuarios será en función de los propietarios de forma aleatoria o simultánea, así también la elaboración de facturas en el caso que fuere necesario y de la recaudación por las ventas de productos o servicios en el transcurso del día.

Se utilizará notas de recepción de equilibrio en todos los equipos y trabajos encomendados, considerando los detalles y características de los mismos, posibles fechas de entrega y fechas de recepción, además de las descripciones de los usuarios. Posterior a esto el equipo pasa al departamento de servicio técnico donde se realizará el cumplimiento o solución del problema detectado con la petición del usuario.

Los trabajos receptados tendrán notas de recepción, por lo que en cada ingreso se tendría en cuenta los detalles y características del mismo, tales descripciones serian: fechas de recepción, fechas de entrega tentativa, datos personales del cliente. Además del proceso el equipo pasara al área de servicio técnico, quienes darán respuesta al usuario.

Al momento de adquirir de repuestos o partes y piezas de los quipos se desarrollan por completo en Babahoyo, ya que en las empresas con mayores importadores de electrónica e informática del Ecuador contamos con contactos comerciales.

Las adquisiciones en su totalidad serán realizadas por medio de facturas legales, permitiendo registrar y controlar los desplazamientos comerciales de la empresa.

El argumento es ocultar las necesidades y ausencias universal de la localidad con relación a lo vinculado con la informática ya que hoy en día, con mayor ímpetu el uso de la tecnología y la informática se han hecho necesarias e indispensables en la productividad de las empresas, con el respectivo almacenamiento de los datos, el trabajo diario, etc.

La percepción es complacer las necesidades de las poblaciones en general sobre lo vinculado con la informática, siendo que hoy en día, más que otras épocas las tecnologías sean utilizadas.

Al considerar que en las ciudades no existe las necesarias empresas que se dedican a esta rama y la necesidad de empresas líderes en todos los servicios, revelan que el total de estos debe ser confiable, puntual, honesto, a precios bajos, justos, con garantía y calidad, eficiencia en todas las prestaciones.

Con la implementación de este análisis de información la empresa COMPUTER S.A de la ciudad de Babahoyo, se brindará la posibilidad de obtener grandes ventajas, incrementar la capacidad de organización en los usuarios, y tomar de esta manera los procesos a una verdadera competitividad, mejorando los reportes de ventas diarias, el control de sus productos, generar una lista de productos por categoría para poder realizar una mejor compra, esta información será sencilla, clara, expedita, veraz, precisa, consistente y fácil de analizar e interpretar. Por todo lo descrito la empresa COMPUTER S.A de la ciudad de Babahoyo, convertirá su emprendimiento

en una verdadera empresa competitiva insertada en el mercado actual, a raíz de los cambios en la economía mundial y la globalización, los datos relativos a todo el proceso productivo de una compañía se han vuelto uno de los elementos fundamentales para lograr el éxito comercial por ello la empresa COMPUTER S.A de la ciudad de Babahoyo. no es ajeno estos cambios, razón fundamental para implementar un análisis de la seguridad informática en la red de datos entre sucursales de la empresa COMPUTER S.A de la ciudad de Babahoyo.

La empresa es la encargada de vender equipos informáticos a los usuarios, así como también les da mantenimiento correctivo y preventivo de las misma para esto realizamos un análisis de la información de los equipos informáticos de los clientes en las diferentes sucursales que tienen disponibles. (ARCERT, 2015, p.5).

La seguridad de información en la red es necesaria, ya que la garantía que se están tratando y comercializando que se está al 100% de control, mientras los datos almacenados como información en el ordenador tienen acceso directo o indirecto a la herramienta Internet, por estar disponible a cualquier hora y día sin limitación y además de ser una de las herramientas más utilizadas a nivel mundial. Para (GARCIA, 2016, p.8) "Internet es la herramienta más práctica, pero a su vez es como la moneda de azar ya que según su uso esta puede ser de fácil manejo en aspecto positivos de la vida, y ser de aprendizaje significativo en cualquier área para el hombre y mujer, como puede destruir y peligrosa para los datos e información personal", las informaciones que pueden quedar desamparadas por el internet pueden ser de carácter personal o empresarial

"Como solución de este problema identificado, se es necesario el diseño y creación de vinculación que permita y de soporte a la actualización de los protectores de los ordenadores ya sean estos virtuales o factibles que puedan dar seguridad a nuestra información y la de los

usuarios, logrando que estos prevean, la disminución de los daños que se pueden suscitar a la información y de esta forma dar protección a los datos de los usuarios y sus PC.” (UCINT, 2012, p.9)

La seguridad de información de la empresa se realiza mediante Nmap (“Network Mapper”) es una herramienta gratuita de código abierto para la exploración de la red o la auditoría de seguridad. Fue diseñado para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. (CRESPO A. , 2015, p. 9) “Utiliza paquetes IP para determinar qué hosts están disponibles en la red, qué servicios (nombre de la aplicación y la versión) estos equipos ofrecen, qué sistemas operativos (y versiones del sistema operativo) se están ejecutando, qué tipo de filtros de paquetes o cortafuegos están en uso, y docenas de otras características”. Nmap se ejecuta en la mayoría de los ordenadores y la consola y versiones gráficas están disponibles. Nmap es libre y de código abierto.

Vulnerabilidades

Los avances de las telecomunicaciones y en los softwares de los equipos han aumentado las amenazas y debilidades que vulneran los sistemas que pueden ser interconectados en diferentes puntos, siendo así el potencial para acceder no autorizado, como fraude o abuso no se limita a un solo punto, sino que puede ocasionar áreas de acceso a la red, lo que diseña nuevas oportunidades y áreas para ingresar a los sistemas. (VITE, 2011, p.12)

El ambiente de internet es un riesgo continuo para las organizaciones que ahora laboran ofreciendo estos servicios. Los riesgos más comunes de los que deben protegerse las instituciones mientras zarpan en internet sus integrantes son los siguientes:

Los Hackers: También se les llama piratas informáticos accedan a la información existente y se transmite por internet, no solo tienen acceso a correos electrónicos si no a ordenadores enlazados a redes perjudicando a las empresas, con el mal uso de la información y su perdida. (CASTRO, 2012, p.48)

Los Cracker: Personas de las que se sabe que intentan romper la seguridad de los sistemas, ingresando con negativas intenciones a la información que mantienen en resguardo las empresas.

Los Virus: Considerados ser programas que alteran o destruyen datos, los mismos que logran ingresar a los sistemas por medio de un dispositivo externo de ingreso de la res, sin necesidad de la manipulación directa del atacante.

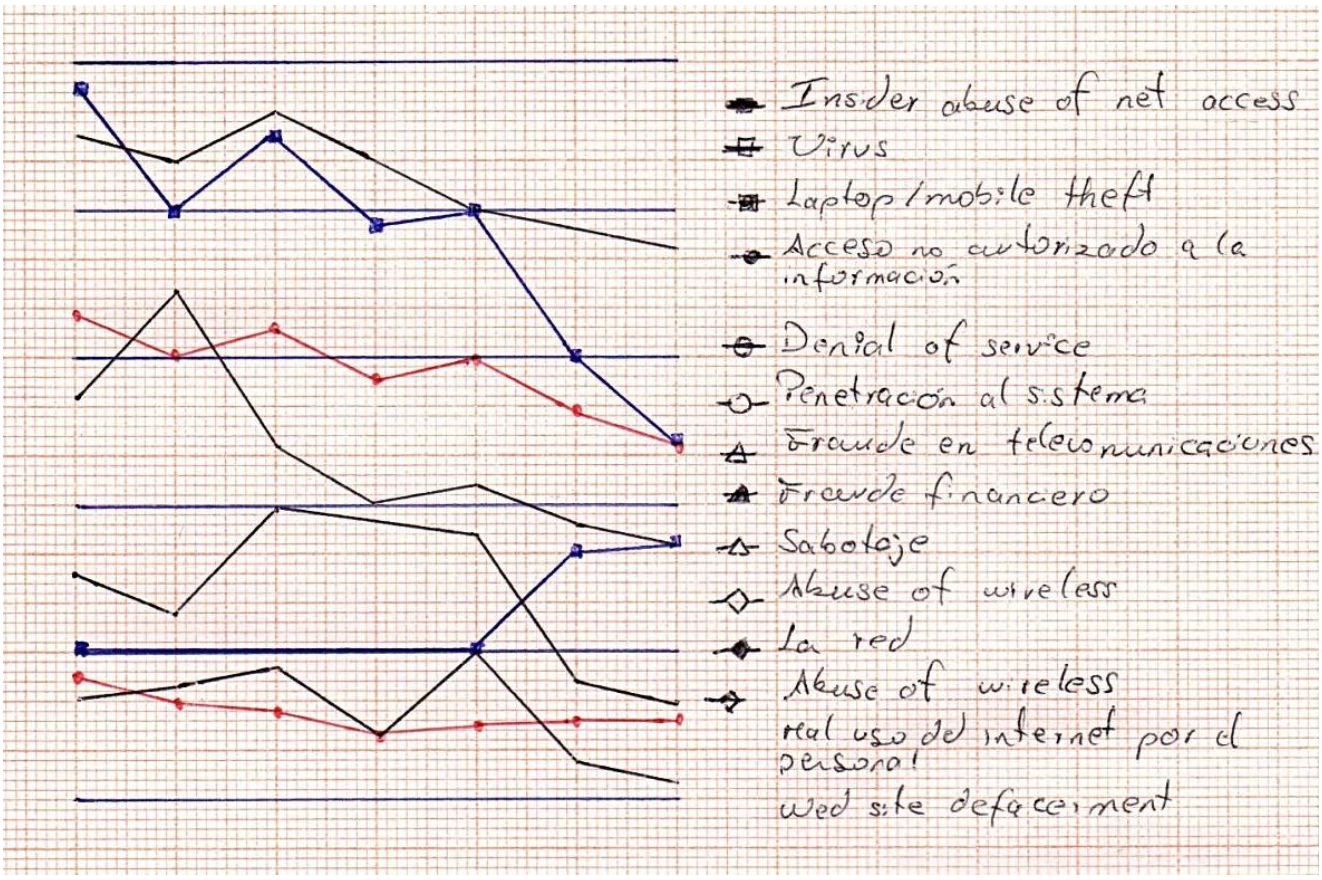
Los Gusanos: Otro tipo de virus que son activados y transmitidos en las redes. Estos tienen como propósito multiplicarse hasta ocupar la mayor cantidad de los discos duros y memorias RAM. Con frecuencia son los ataquen que mayor daño ocasionan ya que con frecuencia generan el colapso de las redes.

Los caballos de Troya: Llamados virus que entran a los ordenadores y posteriormente actúan de manera simultánea a este hecho de la mitología griega. Se aduce a ser un programa inofensivo cuando en la realidad es otra expandiéndose. Son peligrosos cuando son ordenadores de la propia empresa quien se lo instala en programas.

Los Spam: Se los llama también correos no deseados, si bien no se los puede considerar como ataques propiamente dicho, lo cierto es que genera hoy en día perdidas muy millonarias en las empresas u organismos.

Se ha diagnosticado que no solo el internet es una gran amenaza para las empresas, ya que se puede localizar otras tantas en la gestión de la organización. Para (VELASCO, 2014, p. 6) “Entre las amenazas que siempre han estado presentes son el personal de la empresa que por circunstancias llegaría a ser riesgoso por lo que los errores que pueda cometer sin intención como algunos que el principal propósito es ocasionar daños a los documentos digitales de la empresa, un ejemplo caro está el objetivo de imaginar la organización. Uno de los ejemplos como casi contiguo: Claro es cuando en el Departamento de sistema no se genera de los usuarios actividades de los

Figura1: Amenazas/ Ataques detectados entre los años 2015-2016



Fuente: Empresa COMPUTER S.A (2016)

Plan estratégico de seguridad informática

Estos planes estratégicos de seguridad de manera estándar se basan en el conjunto de las políticas de seguridad, luego del resultado de las evaluaciones previas a evaluaciones de los riesgos que reflejen los niveles de seguridad en el que se estén las empresas. (MORA, 2012, p.7)

Evaluación de los riesgos

Se considera como el proceso de evaluación por el cual se logra identificar las vulnerabilidades de la seguridad en las empresas.

Siendo así los objetivos generales de la evaluación de los riesgos son identificados por las causas de los mismos de manera potencial, involucrando a toda las organización, donde no se puede dejar de involucrar los sistemas de información individual, a componentes específicos de sistemas o de servicios, que permitan la factibilidad y cuantificar para que la gerencia cuente con información suficiente y necesaria, con relación a los diseños e implantación de los controles correspondientes con el propósito de disminuir los efectos ocasionados por los riesgos, que se suscitan en los diferentes puntos de análisis. (RAMOS, 2015, p.6)

Figura2: Escala de riesgos R1(Bajo), R2(Medio Bajo), R3(Medio Alto), R4(Alto)

No	Recurso informáticos	R1	R2	R3	R4
1	A	3	3	1	…
2	B	2	2	2	…
3	C	1	1	3	…
4	D	2	4	3	…
2	E	3	2	2	…

Fuente: (MANTÍNEZ, 2012, p. 2)

Políticas de seguridad

Una política de seguridad informática es aquella que fija los lineamientos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen.

Si bien existen algunos modelos o estructuras para su diseño, estás tienen que ser elaboradas de forma personalizada para cada empresa para así recoger las características propias que tiene la organización. (STEPHEN, 2017, p.9)

Una buena política de seguridad corporativa debe recoger, de forma global, la estrategia para proteger y mantener la disponibilidad de los sistemas informáticos y de sus recursos, es decir que estás políticas de seguridad deben abarcar las siguientes áreas.

- Seguridad Física
- Seguridad Lógica
- Seguridad en redes
- Seguridad en los recursos humanos
- Seguridad en el Outsourcing
- Planes de Contingencia

Seguridad en Redes

Las redes y sus seguridades en la información pueden entenderse como la capacidad de las redes o de los sistemas de información para resistir, con determinados niveles de confianza, las acciones malintencionadas y accidentes, que generen peligros en la disponibilidad, integridad, confidencialidad y autenticidad de los datos transferidos y archivados, de los respectivos

servicios que mencionadas redes y sistemas dar o brindan accesibilidad, los mismos que mantienen costos elevados como los ataques intencionados. (ROSS, 2010, p.8).

Dentro de la organización existen redes internas o intranet y las redes externas o extranet que deben ser protegidas de acuerdo a las amenazas a las que cada una está expuesta, estableciendo mecanismos de seguridad contra los distintos riesgos que pudieran atacarlas.

El mantener una red segura fortalece la confianza de los clientes en la organización y mejora su imagen corporativa.

Norma ISO 27001

La ISO 27001 se considera como la norma internacional emitida exclusivamente por la (ISO)Organización Internacional de Normalización

Las normas ISO 27001

ISO 27001 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada.

(CRESPO M. , 2015, p.16) El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información se define como la preservación de:

Confidencialidad. Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

Integridad. Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.

Disponibilidad. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

El objetivo de la norma ISO 27001 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

La norma ISO 27001 establece diez dominios de control que cubren por completo la gestión de la seguridad de la información:

- Política de seguridad.
- Aspectos organizativos para la seguridad.
- Clasificación y control de activos.
- Seguridad ligada al personal.
- Entorno y seguridad física
- Gestión de operaciones y comunicaciones
- Control de los accesos
- Mantenimiento y desarrollo de los sistemas
- Gestión de continuidad del negocio.
- Conformidad con la legislación.

De estos diez dominios se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 127 controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo).

Sistemas informáticos

Las herramientas tales como el internet o el e-mail, son necesarios en las instituciones y puestos de trabajo en las actividades diarias y habituales en el trabajo diario, en la necesidad de dar facilidad en la búsqueda de información, clientes potenciales y proveedores, esto permite una comunicación acelerada tanto dentro como fuera de las organizaciones.

Estos sistemas de gestión de la seguridad en la información (SGSI) son el medio más eficaz de minimizar los riesgos, (MANTÍNEZ, 2012, p. 2). "Luego de realizar la aseguración que se identifican y valoran los activos y los riesgos, se consideran de gran impacto para las empresas, y se adoptan los controles y procesos más coherentes y eficientes con las estrategias de negocios".

Las gestiones efectivas de la seguridad en la información permiten las garantías:

Su confidencialidad, se segura que solo aquellos que están autorizados ingresen a la información.

La integridad, es asegurar que los datos e información almacenada y sus métodos de gestión son exactos completos y la identidad asegurando que los clientes con autorización tengan acceso a la información y datos de los activos relacionados cuando lo necesiten.

Datos y redes

El termino de redes proviene del latín. Más con claridad se emana del vocablo "rete", que es sinónimo de malla.

Política de seguridad

Dirigir y dar soporte a la gestión de la seguridad de la información.

La alta dirección debe definir una política que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicitarla de la forma adecuada a todo el personal implicado en la seguridad de la información. (BARATTA, 2014, p.2)

La política se constituye en la base de todo el sistema de seguridad de la información. Y la alta dirección debe apoyar visiblemente la seguridad de la información en la compañía.

Alcance

El diseño de políticas de seguridad informática planteadas a partir de los resultados del análisis de riesgo cuyos factores de riesgo son el resultado de las evaluaciones a las seguridades de la entidad y fundamentadas en las normas y/o estándares de seguridad informática.

Estas políticas serán puestas en práctica por la empresa mediante la ejecución del diseño del plan estratégico de seguridad que será desarrollado para ser aplicado.

El diseño de este plan estratégico trata de cubrir los objetivos que la empresa está en capacidad de llevar a cabo para disminuir los riesgos a los que está expuesta.

Este plan de seguridad servirá como una guía aplicable a cualquier otra empresa y podrá ser implementado en toda la organización, pero deberá ser dirigido por el Jefe de Seguridad y a falta de este el Jefe de Sistemas; el cual se hará responsable de que dichas políticas de seguridad sean cumplidas a cabalidad por todos los integrantes de la compañía.

CONCLUCIONES

- Este proyecto de desarrollo de un Sistema de Información comprende varios componentes o pasos llevados a cabo durante la etapa del análisis, el cual ayuda a traducir las necesidades del cliente en un modelo de Sistema que utiliza uno más de los componentes: Software, hardware, personas, base de datos, documentación y procedimientos.

- En conclusión la seguridad informática se encarga de proteger todo lo relacionado con la infraestructura computacional y la información que se encuentra en las computadoras, existen varias amenazas por lo que se debe tener cuidado con lo que se abre en internet y en correos que mandan personas desconocidas, ya que, es posible que la computadora sea infectada con un virus y traiga problemas a esta, tales como la pérdida total o parcial de la información, falsificación de los datos, interferencia en el funcionamiento, etc. Pero el número de amenazas se pueden reducir si se coloca un antivirus y si se evita entrar en páginas o correos electrónicos que aparenten ser extraños

- Debido a la constante amenaza en que se encuentran los sistemas, es necesario que los usuarios y las empresas enfoquen su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos que luego se pueden traducir en grandes pérdidas.

BIBLIOGRAFÍA

ARCERT, C. (2015, p.5). *servidores web.*

BARATTA, A. (2014, p.2). Seguridad . *Seguridad. Capítulo criminológico*, p.2.

CASTRO, B. (2012, p.48). *peligros más frecuentes de los que deben protegerse las empresa.*

CRESPO, A. (2015, p. 9). *seguridad de información de la empresa.*

CRESPO, M. (2015, p.16). *ISO 27001*. Encuesta ISO sobre certificaciones de la norma para sistemas de gestión.

GARCIA, A. (2016, p.8). *Problematica de un sistema de de la seguridad in formatica.*

kurose Ross. (2010). *www.informaticaitc.com/consultoria-informatica/seguridad.* http://www.jprenafeta.com/areas-de-practica/uso-de-herramientas-informaticas-en-la-empresa/.

MANTÍNEZ, A. (2012, p. 2). Auditoría con Informática a Sistemas Contables. *Revista de Arquitectura e Ingeniería*, 2.

MORA, S. (2012, p.7). *www.dte.us.es/personal/mcromero/docs/ip/tema-seguridad-IP.pdf.*

RAMOS, V. (2015, p.6). *www.gestiopolis.com/administracion-de-redes-y-seguridad-inform...*

ROSS, k. (2010, p.8). *Seguridad en redes.* Argentina: Ed. Los Angeles.

STEPHEN, W. (2017, p.9). Seguridad en auditoria. *Revista Seguridad*, 9.

UCINT, G. (2012, p.9). *Definición s de seguridad para proteger infraestructuras críticass.*

VELASCO, P. (2014, p. 6). *www.redeszone.net/seguridad-informatica/.*

VITE, R. (2011, p.12). *vulnerabilidades de taques informaticos.*

ANEXOS

UNIVERSIDAD TECNICA DE BABAHOYO

Encuesta del informe del estudio de caso del tema: Análisis de la seguridad informática en la red de datos entre sucursales de la empresa COMPUTER S.A. de la ciudad de Babahoyo.

1) ¿Qué herramientas de seguridad usted recomienda para pequeñas empresas?
___ Antivirus, Antispywarer, Antimalware
___ Firewall
___ Políticas de seguridad

2) ¿Cuál sería el mecanismo eficiente para realizar el seguimiento de los equipos que forman parte de la red?
___ Sistema automatizado
___ Inventario
___ A través de una bitácora de control

3) ¿Qué tipo de políticas o normas de seguridad informática usted recomienda aplicar?
___ Seguridad de la información (Seguridad)
___ ISO 27000 (Seguridad)
___ ISOMEC 27001 (Mejora continua)

4) ¿Qué tipo de mecanismos usted recomienda para poder evaluar políticas o normas de seguridad?
___ Aplicativo adaptado o enfocado a este fin
___ Sub contratación encargada de llevar este control
___ Ningún tipo de sistemas de evaluación

5) ¿Cómo usted recomienda llevar el proceso de control de los mecanismos de seguridad?
___ No es necesario
___ Aplicación adaptada
___ Personal interno

6) ¿Cómo recomendaría usted poder validar y evaluar el rubro de la seguridad informática en una red?
___ Por sistema ligero
___ Por subcontratación
___ Manual de registro

7) ¿Si usted se enfoca a manejar la seguridad con una herramienta como preferiría que fuese esta herramienta a nivel de licencias o pago?
___ Con licencia
___ Gratuita
___ De prueba

Análisis de datos

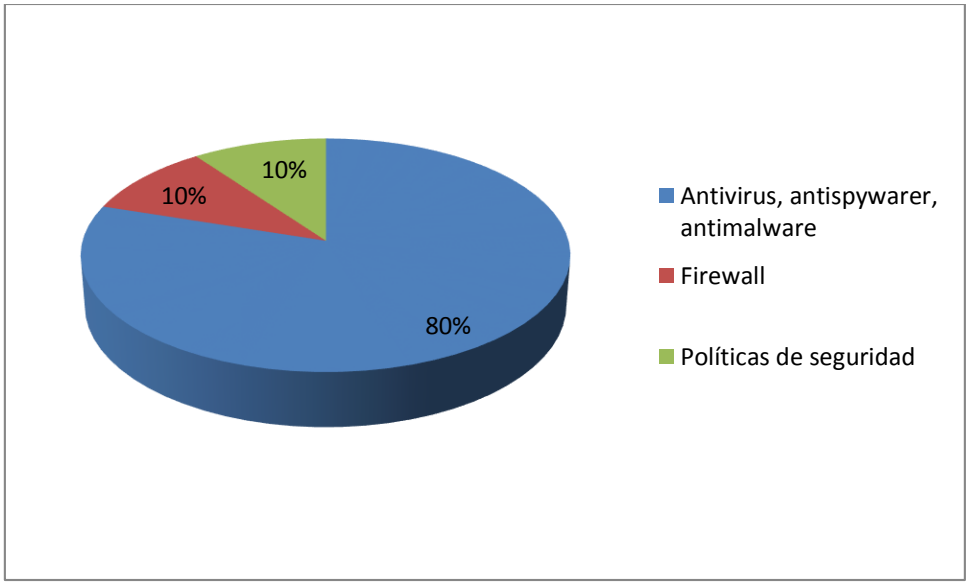
1) ¿Qué herramientas de seguridad usted recomienda para pequeñas empresas?

Cuadro Nº 1

Detalle	Cantidad	Frecuencia
Antivirus, Antispywarer, Antimalware	16	80%
Firewall	2	10%
Políticas de seguridad	2	10%
Total	20	100%

Fuente: Empleados de la empresa COMPUTER S.A. de la ciudad de Babahoyo
Elaboración: Por la autora

Gráfico Nº 1



Fuente: Empleados de la empresa COMPUTER S.A. de la ciudad de Babahoyo
Elaboración: Por la autora

Análisis: De los encuestados el 80%, manifiestan que las herramientas que recomiendan para las pequeñas empresas con Antivirus, Antispywarer, Antimalware, el 10% indican Firewall y el otro 10% Políticas de seguridad.

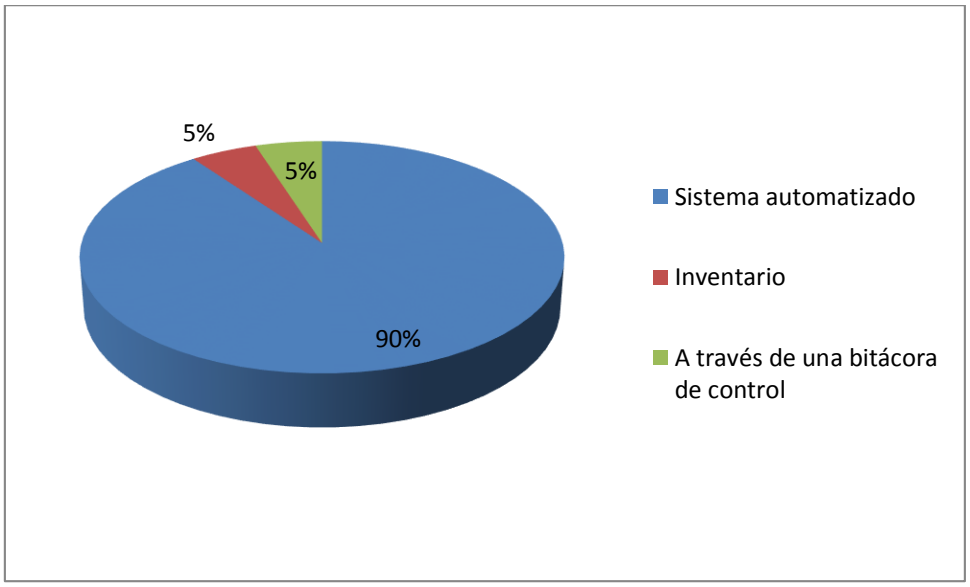
2) ¿Cuál sería el mecanismo eficiente para realizar el seguimiento de los equipos que forman parte de la red?

Cuadro Nº 2

Detalle	Cantidad	Frecuencia
Sistema automatizado	18	90%
Inventario	1	5%
A través de una bitácora de control	1	5%
Total	20	100%

Fuente: Empleados de la empresa COMPUTER S.A. de la ciudad de Babahoyo
Elaboración: Por la autora

Gráfico Nº 2



Fuente: Empleados de la empresa COMPUTER S.A. de la ciudad de Babahoyo
Elaboración: Por la autora

Análisis: De los encuestados el 90% manifestaron que el mecanismo eficiente sería un sistema automatizado, mientras que el 5% que los inventarios y otro 5% que una bitácora.

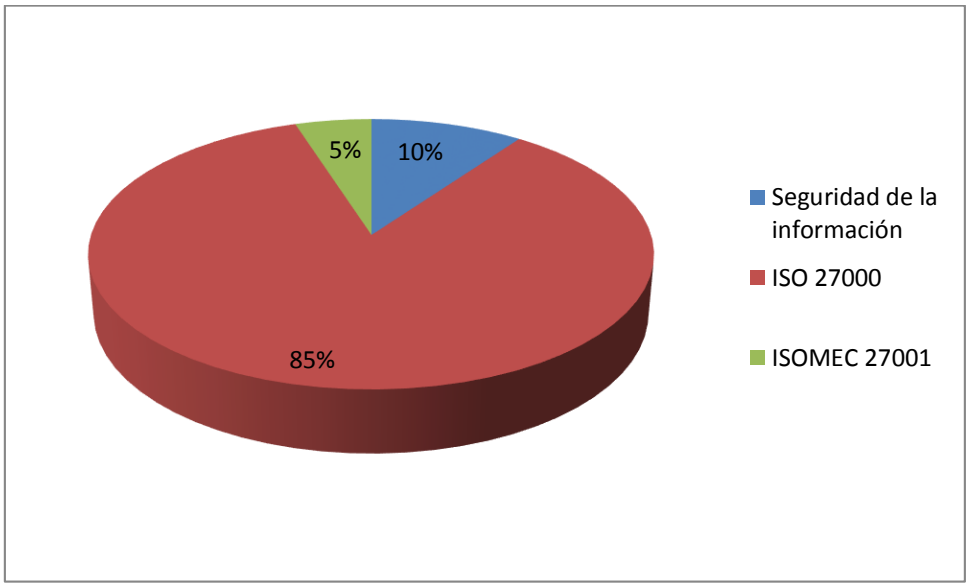
3) ¿Qué tipo de políticas o normas de seguridad informática usted recomienda aplicar?

Cuadro Nº 3

Detalle	Cantidad	Frecuencia
Seguridad de la información	2	10%
ISO 27000	17	85%
ISOMEC 27001	1	5%
Total	20	100%

Fuente: Empleados de la empresa COMPUTER S.A. de la ciudad de Babahoyo
Elaboración: Por la autora

Gráfico Nº 3



Fuente: Empleados de la empresa COMPUTER S.A. de la ciudad de Babahoyo
Elaboración: Por la autora

Análisis: Con el 10% los empleados respondieron que la seguridad de la información, el 85% que la ISO 27000 y el 5% que es ISOMEC 27001.

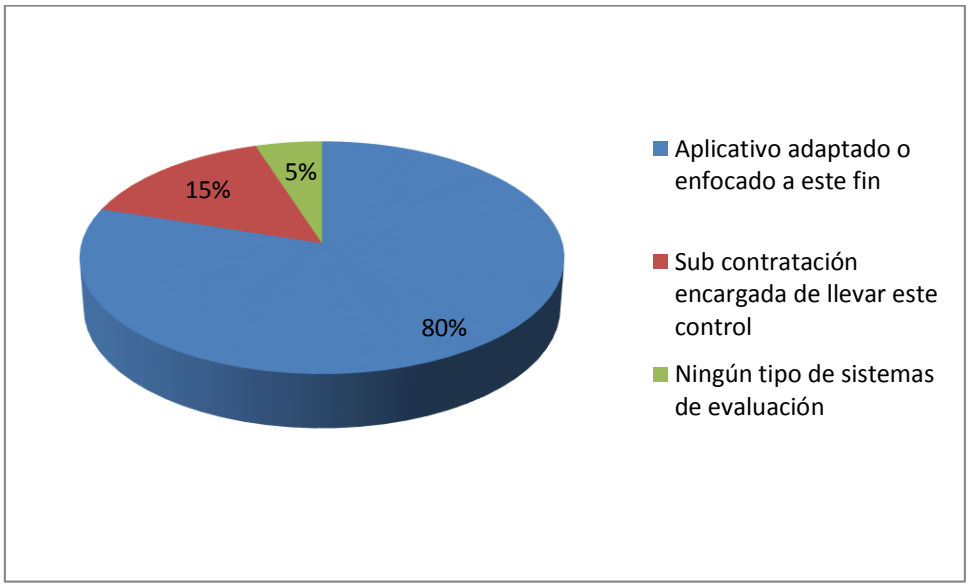
4) ¿Qué tipo de mecanismos usted recomienda para poder evaluar políticas o normas de seguridad?

Cuadro Nº 4

Detalle	Cantidad	Frecuencia
Aplicativo adaptado o enfocado a este fin	16	80%
Sub contratación encargada de llevar este control	3	15%
Ningún tipo de sistemas de evaluación	1	5%
Total	20	100%

Fuente: Empleados de la empresa COMPUTER S.A. de la ciudad de Babahoyo
Elaboración: Por la autora

Gráfico Nº 4



Fuente: Empleados de la empresa COMPUTER S.A. de la ciudad de Babahoyo
Elaboración: Por la autora

Análisis: Con el 80% aplicativo adaptado o enfocado a este fin, sub contratación encargada de llevar este control el 15% y ningún tipo de sistemas de evaluación el 5%.

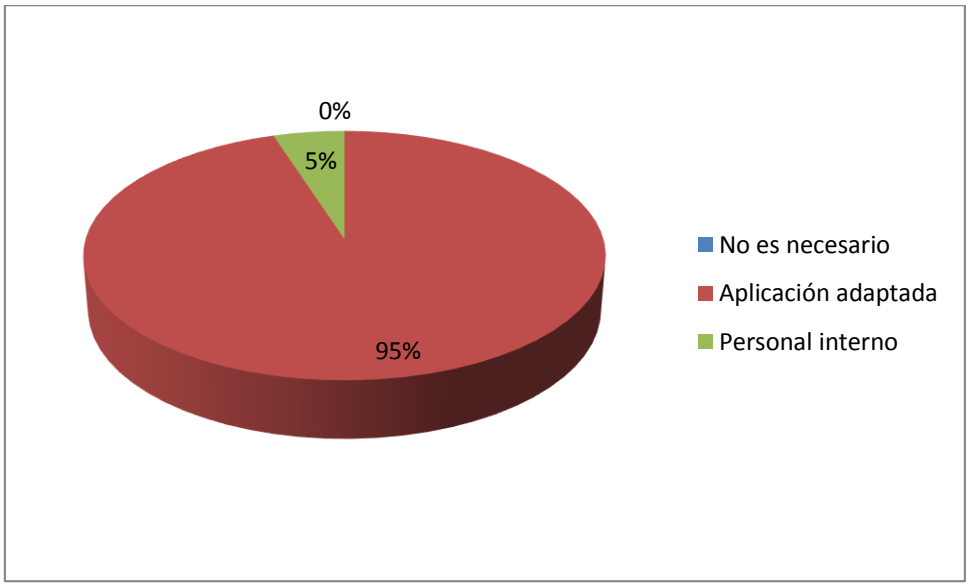
5) ¿Cómo usted recomienda llevar el proceso de control de los mecanismos de seguridad?

Cuadro Nº 5

Detalle	Cantidad	Frecuencia
No es necesario	0	0%
Aplicación adaptada	19	95%
Personal interno	1	5%
Total	20	100%

Fuente: Empleados de la empresa COMPUTER S.A. de la ciudad de Babahoyo
Elaboración: Por la autora

Gráfico Nº 5



Fuente: Empleados de la empresa COMPUTER S.A. de la ciudad de Babahoyo
Elaboración: Por la autora

Análisis: De los encuestados el 95% debe ser aplicación adaptada y el 5% por personal interno.

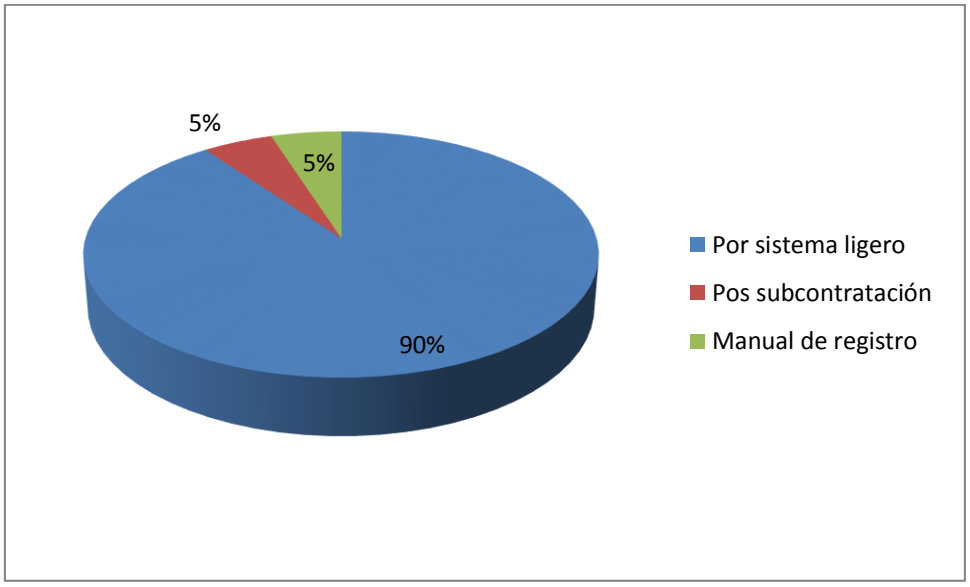
6) ¿Cómo recomendaría usted poder validar y evaluar el rubro de la seguridad informática en una red?

Cuadro Nº 6

Detalle	Cantidad	Frecuencia
Por sistema ligero	18	90%
Sub contratación	1	5%
Manual de registro	1	5%
Total	20	100%

Fuente: Empleados de la empresa COMPUTER S.A. de la ciudad de Babahoyo
Elaboración: Por la autora

Gráfico Nº 6



Fuente: Empleados de la empresa COMPUTER S.A. de la ciudad de Babahoyo
Elaboración: Por la autora

Análisis: Con el 90% se considera que es sistema ligero, con el 5% de respuesta Sub contratación y otro 5% por manual de registro.

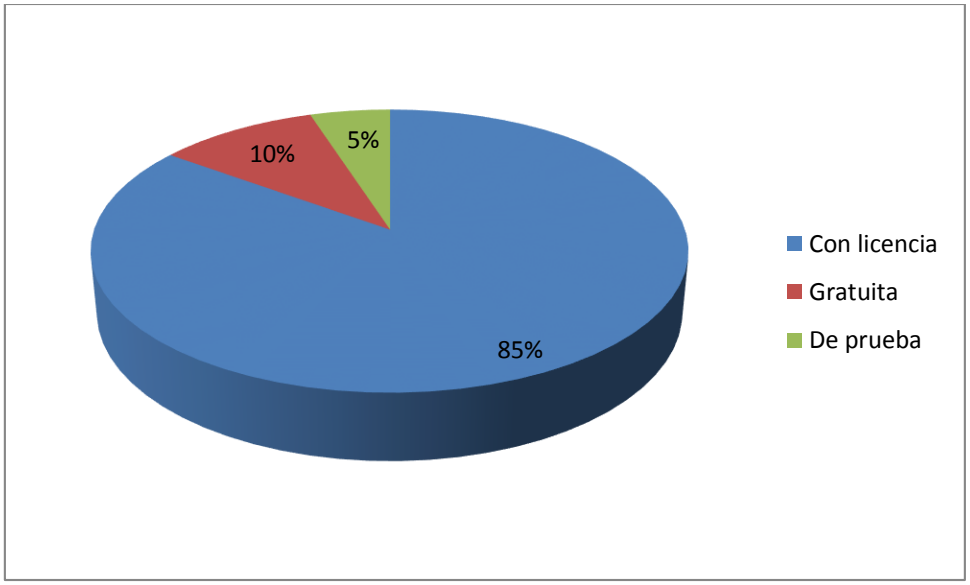
7) ¿Si usted se enfoca a manejar la seguridad con una herramienta como preferiría que fuese esta herramienta a nivel de licencias o pago?

Cuadro Nº 7

Detalle	Cantidad	Frecuencia
Con licencia	17	85%
Gratuita	2	10%
De prueba	1	5%
Total	20	100%

Fuente: Empleados de la empresa COMPUTER S.A. de la ciudad de Babahoyo
Elaboración: Por la autora

Gráfico Nº 7



Fuente: Empleados de la empresa COMPUTER S.A. de la ciudad de Babahoyo
Elaboración: Por la autora

Análisis: De los encuestados el 85% con licencia, el 10% gratuita y el 5% de prueba debe ser.

UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

UNIDAD DE TITULACIÓN

SEGUIMIENTO AL TRABAJO DE TITULACIÓN

ESCUELA: Carrera de Ingeniería en Sistemas
Fecha de presentación: 28 de Agosto del 2017
MODALIDAD: Examén Complexivo - Caso de Estudio
EGRESADO: Iraida Graciela Lima Cerna
DOCENTE: Ing. Joffre Vicente León Acurio
TEMA: Análisis de la seguridad informática en la red de datos entre sucursales de la empresa COMPUTER S.A de la ciudad de Babahoyo.

FECHA	ACTIVIDAD	LOGRO	PROXIMA ACTIVIDAD	FIRMAS DE LOS RESPONSABLES
09/03/2017 13-03-2017	• Se revisó el tema del Caso de Estudio y la pertinencia de dicho trabajo de investigación. • Se realizaron cambios al tema. • Se determinó la línea y sub-línea de investigación	10%		
20-03-2017 27-03-2017	• Se realizaron ajustes a los antecedentes, propósito de estudio (objetivo). • Planteamiento de la pregunta de reflexión. • Se compartió un formato de caso de estudio a trabajar	25%		
03-04-2017 10-04-2017	• Se revisó la Unidad de Análisis (Marco Conceptual). • Se verificó que el trabajo esté referenciado y aplicado las normas APA.	50%		
17/04/2017 24-04-2017	• Se revisó los avances en el trabajo metodológico y recolección de información. • Se analizó la interpretación de resultados y análisis de la información	70%		
08/05/2017	• Se comprobó los cambios realizados en el análisis de la información obtenida, se validó los resultados obtenidos con las conclusiones	90%		
01/06/2017	• Se revisó el trabajo Caso de Estudio completo y normalizado con APA 6v.	100%		

UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
COMISIÓN DE INVESTIGACIÓN CIENTIFICA
UNIDAD DE TITULACIÓN

Babahoyo, 28 de agosto de 2017

Sr. CPA.
Julio Mora Aristega
COORDINADOR DE LA UNIDAD DE TITULACIÓN DE LA FAFI – UTB
En su despacho.-

De mi consideración:

En atención a la designación como docente – tutor para guiar el estudio de caso del Sr. (Srta.) **IRAIDA GRACIELA LIMA CERNA** titulado **Análisis de la seguridad informática en la red de datos entre sucursales de la empresa COMPUTER S.A de la ciudad de Babahoyo.**
Al respecto tengo a bien informar lo siguiente:

1. El trabajo está relacionado con las sublíneas de investigación de la carrera.
2. La información es suficiente y pertinente.
3. La parte metodológica y bibliográfica es adecuada.
4. Cumple con la normativa Apas, reglas de ortografía sintaxis y gramática.

Por lo anteriormente expuesto, el estudio de caso es aprobado por quien suscribe, autorizando su exposición ante el tribunal que se designe para el efecto.

Por la atención que se sirva dar al presente me suscribo.

Atentamente

Joffre Vicente León Acurio
EQUIPO DE TITULACIÓN FAFI - UTB